МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографические протоколы»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

Основной целью изучения дисциплины «протоколы» является формирование у обучающегося компетенций для следующих видов деятельности:
контрольно-аналитическая;
эксплуатационная.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
Контрольно-аналитическая деятельность:
-предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
-подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.
Эксплуатационная деятельность:
-установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;
-установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;
-проверка технического состояния и профилактические осмотры технических средств защиты информации;
-проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Дисциплина «Криптографические протоколы» имеет целью ознакомление слушателей существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.
Задача дисциплины «Криптографические протоколы» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.
Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: применение стандартных криптопротоколов и интернет-технологий, средств и методов хранения и передачи аутентификационной информации, основных протоколов идентификации и аутентификации абонентов, протоколов дистанционного принятия решений, математических моделей шифров, использование криптографических стандартов.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Криптографические протоколы" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-6	Способен анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, средств технической защиты информации, сетей и систем передачи информации при решении профессиональных задач
ОПК-8	Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям
ОПК-10	Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях
ОПК-17	Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях
ПКО-6	Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПКО-11	Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Криптографические протоколы» осуществляется в форме лекций, практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100% являются традиционными классически-лекционными (объяснительно-иллюстративные). Практические занятия также организованы в традиционной классно-урочной организационной форме, с использованием технологий развивающего обучения. Также предполагается, что студенты могут делать небольшие 15-20-минутные доклады-презентации по разбираемым темам (возможны видеоконференции при подготовке докладов). Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных лабораторных заданий с использованием..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Понятие протокола, виды протоколов.
Контрольная работа

Тема: Понятие протокола, отличия от криптосистем, примеры.

Тема: Цели и предназначение протоколов.

Тема: Криптостойкость протоколов.

Тема: Виды криптокпротоколов.

Тема: Протоколы с нулевым разглашением.

Тема: Аутентификация в информационных системах.

РАЗДЕЛ 2
Стандарт. Криптопротоколы.
Контрольная работа

Тема: Протокол Диффи-Хеллмана.

Тема: Протокол Блюма.

Тема: Протокол аутентификации Шнорра.

Тема: Электронная подпись RSA.

Тема: Крипт. хэш-функции.

Тема: Электронная подпись Шнорра.

РАЗДЕЛ 3
Другие виды криптопротоколов.

Тема: Протоколы, связанные с электронными платежами.

Тема: Электронные купюры.

Тема: Электронные деньги одного номинала.

Тема: Электронные деньги разного номинала.

Тема: Разделение секрета.

Тема: Протоколы голосования.

Экзамен